

# Prescriptions techniques relatives aux échanges de données entre le téléservice « reseaux-et-canalisation.s.gouv.fr » et ses partenaires

N° DSI-09-103308-11966D

INERIS  
Verneuil en Halatte


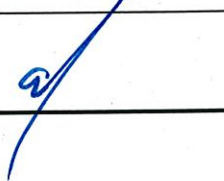
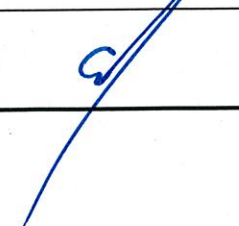
6 juin 2011



## PRÉAMBULE

Le présent document expose les prescriptions techniques relatives aux échanges de données entre d'une part le guichet unique et d'autre part les exploitants de réseaux et les prestataires d'aide à la réalisation des déclarations de projet de travaux (DT) et d'intention de commencement de travaux (DICT).

Il est pris notamment en application de l'article 7 de l'arrêté du 23 décembre 2010, relatif aux obligations des exploitants d'ouvrages et des prestataires d'aide envers le téléservice « [reseaux-et-canalizations.gouv.fr](http://reseaux-et-canalizations.gouv.fr) ».

	<b>Rédaction</b>	<b>Vérification</b>	<b>Approbation</b>
<b>NOM</b>	Carine Louvion	Michel Treins	Michel treins
<b>Qualité</b>	Chef de projet	Directeur des systèmes d'information	Directeur des systèmes d'information
<b>Visa</b>			

## TABLE DES MATIÈRES

<b>1. IDENTIFICATION, TRAÇABILITE ET SIGNATURE .....</b>	<b>5</b>
1.1 Echanges dématérialisés devant être sécurisés .....	5
1.1.1 Cadre législatif et réglementaire .....	6
1.2 La signature électronique .....	7
1.2.1 Caractéristiques d'une signature électronique .....	7
1.2.2 Notion de « signature (ou cachet) serveur » .....	7
1.2.3 Le certificat électronique.....	7
1.2.4 Les services de confiance complémentaires .....	8
1.2.4.1 Horodatage.....	8
1.2.4.2 Gestion de la preuve .....	9
1.2.5 Signature certifiée .....	9
1.3 Préconisations.....	10
1.3.1 Normes et standards utilisés dans les produits de sécurité.....	10
1.3.2 Documents et informations délivrés par le guichet unique en réponse à une demande de renseignement.....	10
1.3.3 Cas des Déclarants .....	11
1.3.4 Cas des prestataires d'aide .....	11
1.3.5 Cas des exploitants et propriétaires d'ouvrages .....	12
<b>2. GESTION DES REFERENTIELS .....</b>	<b>13</b>
2.1 Géocodage.....	13
2.2 Mise à jour des données de zonage des exploitants.....	14
<b>3. FLUX, PROTOCOLES D'ECHANGE, FORMATS DE DONNEES .....</b>	<b>15</b>
3.1 Diagramme des flux.....	15
3.2 Flux identifiés pour les prestataires d'aide .....	17
3.2.1 Macro-flux A - Flux entre le déclarant et le téléservice.....	17
3.2.1.1 Flux A.1 – Requête d'un déclarant .....	17
3.2.1.2 Flux A.2 - Téléchargement sécurisé de la liste des exploitants signée et horodatée.....	18
3.2.2 Macro-flux B - Echange entre les serveurs web et le service de base de données .....	18
3.2.2.1 Flux B.1 - Connexion aux services de bases de données du guichet unique.....	19
3.2.2.2 Flux B.2 - Echange d'information avec les services de bases de données .....	20
3.2.2.3 Flux B.3 - Intervention des prestataires d'aide sur le guichet unique.....	22
3.2.2.4 Flux B.4 – Tunnelisation entre le guichet unique et les prestataires d'aide .....	23
3.2.3 Macro-flux C - Informations échangées avec un organisme tiers archiveur .....	23
3.2.3.1 Flux C.1 - Tunnelisation avec le tiers archiveur .....	24
3.2.3.2 Flux C.2 - Archivage des dossiers de preuve électronique.....	25
3.3 Flux identifiées pour l'exploitant de reseaux .....	25
3.3.1 Macro-flux n° D - Mise à jour des données des exploitants .....	25
3.3.1.1 Flux D.1 – Mise à jour manuelle des données par l'exploitant.....	26
3.3.1.2 Flux D.2 – Mise à jour des données de l'exploitant par upload de fichier .....	27
3.3.1.3 Flux D.3 – Autre cas : Impossibilité de mise à jour directe ou d'utiliser le mode lot.....	29
<b>4. INDEX DES FIGURES ET DES TABLEAUX.....</b>	<b>30</b>

## 1. IDENTIFICATION, TRAÇABILITE ET SIGNATURE

### 1.1 ECHANGES DEMATERIALISES DEVANT ETRE SECURISES

Les échanges concernés sont, *au minimum*, les suivants :

- Sessions sécurisées entre le site internet du guichet unique et un déclarant :
  - Documents et données adressés aux déclarants, lors d'une demande de renseignements effectuée par ces derniers en vue de remplir leurs obligations réglementaires préalables à la réalisation de travaux.
- Sessions sécurisées entre le site internet du guichet unique et une personne physique, travaillant chez un exploitant de réseau, ou chez un prestataire:
  - Mise à jour, par saisie, des coordonnées des exploitants et/ou propriétaires d'ouvrages.
  - Suivi et reporting adressés aux exploitants en retour des procédures d'importation et de traitement des leurs données.
  - Activités de consultation, de supervision, de remontées d'informations (Journal récapitulatif des consultations effectuées sur leur site internet) et de paramétrage effectuées par les prestataires d'aide ayant passé convention avec le guichet unique.
- Sessions sécurisées entre une personne physique du guichet unique et une personne physique : déclarant, personnel d'un exploitant / propriétaire d'ouvrage, ou personnel d'un prestataire d'aide :
- Sessions sécurisées entre les serveurs du guichet unique et ceux des exploitants et/ou propriétaires de réseaux :
  - Procédures d'importation des données fournies à des fins d'enregistrement par les exploitants et/ou propriétaires d'ouvrages.
- Sessions sécurisées entre les serveurs du guichet unique et ceux des prestataires d'aide :
  - Requêtes / réponses directes entre les systèmes de bases de données du guichet unique et les systèmes d'information des prestataires d'aide.
  - Synchronisation des bases de données du guichet avec les réplicas partiels ou totaux mis en œuvre par les prestataires d'aide.

La sécurisation des échanges permet de répondre aux exigences suivantes :

- Intégrité des données échangées qui ne peuvent pas être modifiées durant leur transfert.
- Non répudiation des données envoyées et/ou reçues : l'expéditeur et/ou le destinataire ne peuvent contester l'envoi / la réception des informations.
- Confidentialité, le cas échéant, des données, qui ne doivent pouvoir être lues que par leurs destinataires autorisés.
- Authentification de l'identité du ou des interlocuteurs, de façon non ambiguë.

La sécurisation s'appuie sur deux démarches principales :

1. La signature électronique, y compris l'identification et l'authentification des signataires ;
2. Le recours à des services de confiance complémentaires : horodatage, création, séquestre, et archivage de preuve électronique, validation de signature, validation de certificat, etc.

### **1.1.1 CADRE LEGISLATIF ET REGLEMENTAIRE**

Ces actions s'inscrivent dans le cadre législatif et réglementaire suivant :

- La directive européenne n°1999/93/CE du 13 décembre 1999 sur la signature électronique.
- Sa transposition en droit français par la loi n°2000-230 du 13 mars 2000 et son décret d'application n°2001-272 du 30 mars 2001. La loi, en modifiant l'article 1316 du Code civil, pose le principe de la validité juridique de la signature électronique.
- Le décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
- La décision de la commission européenne du 14 juillet 2003 relative à la publication des numéros de référence de normes généralement admises pour les produits de signature électroniques conformément à la directive 1999/93/CE citée précédemment.
- La loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
- L'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.
- La loi n°2004-1343 du 9 décembre 2004 de simplification du droit. Cette loi, en son article 3, a autorisé le gouvernement à prendre par ordonnance les mesures nécessaires pour assurer la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives.
- L'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- *Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.* portant notamment sur les points suivants (liste non exhaustive) :
  - le Référentiel Général de Sécurité (RGS),
  - la qualification des produits de sécurité,
  - la qualification des Prestataires de Services de Confiance (PSCo),
  - la validation des certificats électroniques par l'Etat,
  - le référencement des produits de sécurité et des PSCo.

Sont concernés par l'ordonnance tous les services publics administratifs de l'Etat, et tous les organismes (de droit public ou de droit privé) chargés de la gestion d'un service public.

Le Référentiel Général de Sécurité comprend un ensemble de règles que doivent respecter certaines fonctions contribuant à la sécurité des informations échangées par les autorités administratives avec les usagers ou entre elles. Le RGS reprend et complète les recommandations « PRIS » (Politique de Référencement Intersectorielle de Sécurité), aujourd'hui en V2.2.

## 1.2 LA SIGNATURE ELECTRONIQUE

### 1.2.1 CARACTERISTIQUES D'UNE SIGNATURE ELECTRONIQUE

Une signature électronique, pour être probante, doit présenter les caractéristiques suivantes :

1. Elle est liée uniquement au signataire ;
2. Elle permet d'identifier le signataire ;
3. Elle est créée par des moyens que le signataire conserve sous son contrôle exclusif ;
4. Elle est liée au message auquel elle se rapporte, de telle sorte que son intégrité est garantie, et que toute modification ultérieure soit détectable.

### 1.2.2 NOTION DE « SIGNATURE (OU CACHET) SERVEUR »

Dans le cas de téléservices tels que le guichet unique, faisant intervenir non pas des personnes physiques, mais des systèmes applicatifs fonctionnant sur des machines ou des groupes de machines, la signature électronique est réalisée par un élément matériel ou logiciel, et non pas par un être humain. Or, comme seule une personne physique peut signer, au sens juridique du terme, cette opération prend ici le nom de « cachet serveur ».

Un « cachet serveur » permet de garantir l'intégrité des données et d'identifier de façon non ambiguë les serveurs ayant cacheté (signé) les données.

### 1.2.3 LE CERTIFICAT ELECTRONIQUE

Un certificat électronique fait la preuve, avec un niveau de confiance suffisant, de l'identité du signataire. Il permet d'associer, de façon sûre, une bi-clé d'authentification ou de signature à une identité (personne physique ou élément matériel et logiciel).

Dans ce but, il est délivré par une autorité de certification (AC), à l'issue d'une procédure de vérification de l'identité<sup>1</sup> faite par une autorité d'enregistrement (AE)<sup>2</sup> : par exemple, rencontre face à face, vérification des pièces d'identité, ou encore, communication d'un élément propre au porteur, permettant de l'identifier au sein d'une base de données administrative préétablie.

La structure des certificats est établie de façon normative (norme X509 V3) par l'Union Internationale des Télécommunications (UIT), organisme dépendant des Nations Unies.

---

<sup>1</sup> Ces procédures sont habituellement référencées au sein d'une **politique de certification (PC)** et d'une **déclaration des pratiques de certification (DPC)**, élaborées et maintenues par l'organisme certificateur.

<sup>2</sup> Les deux autorités sont fréquemment opérées par une même organisation.

Le certificat est lui-même signé par l'autorité qui l'a établi. Il comporte donc également les informations permettant de vérifier cette signature.

Le certificat peut être révoqué à tout moment par l'autorité émettrice (par exemple, en cas de compromission de la clé). Par conséquent, lorsqu'il reçoit des informations signées, le destinataire doit vérifier, à l'aide d'outils informatiques, la validité du certificat. Cette vérification peut être effectuée de deux façons :

1. En consultant *des listes de révocation*<sup>3</sup> publiées à intervalle régulier par l'autorité de diffusion associée à l'AC.
2. En effectuant une requête directe auprès des systèmes informatiques de cette dernière, selon un protocole standardisé de l'IETF<sup>4</sup> (RFC 2560), appelé OCSP « Online Certificate Status Protocol ».

Un certificat et sa bi-clé sont généralement réservés à un usage unique : signature, authentification, chiffrement... Seul le double usage authentification et signature est toléré pour certains types de certificats.

Dans le cadre de l'authentification d'un message ou de données, l'authentification est réalisée en appliquant une transformation cryptographique identique à la signature électronique.

Le service d'authentification permet de garantir l'intégrité et l'origine du message / des données authentifiées mais, contrairement au service de signature électronique, il ne signifie pas que l'émetteur manifeste son consentement sur le contenu du message ou des données.

#### **1.2.4 LES SERVICES DE CONFIANCE COMPLEMENTAIRES**

Des services de confiance complémentaires sont nécessaires pour renforcer la force probante de la signature. Parmi ceux-ci, on citera principalement :

##### **1.2.4.1 HORODATAGE**

L'horodatage consiste à associer à un document ou un message, la date et l'heure exacte d'une transaction, telle que la signature électronique, l'envoi, la réception, le téléchargement, l'ouverture...

L'horodatage permet :

- De donner une date et une heure fiable à l'opération de signature électronique du document, renforçant ainsi son caractère non répudiable.
- De s'assurer que le certificat de signature était bien valide lors de l'opération de signature.
- D'établir les conditions favorables à la création d'un dossier de preuve et d'un archivage légal.

Le tampon d'horodatage est fourni par un tiers horodateur, qui peut être un prestataire extérieur ou bien l'autorité administrative elle-même si elle décide de gérer elle-même le service dans des conditions permettant d'en garantir la qualité et la sécurité. L'horodatage est décrit de façon standardisée par la RFC 3161 de l'IETF.

---

<sup>3</sup> CRL – Certificate Revocation List

<sup>4</sup> Internet Engineering Task Force - est un groupe informel, sans statut, sans membre, sans adhésion. Le travail technique est accompli dans une centaine de groupes de travail.



#### 1.2.4.2 GESTION DE LA PREUVE

Un dossier de preuves comporte, outre le document lui-même, tous les éléments permettant une restitution fidèle de la transaction : la chaîne de confiance des certificats, les différentes signatures, les jetons d'horodatages, les listes de révocation en vigueur au moment de la signature ou les jetons OSCP attestant d'une vérification en ligne du statut des certificats, etc.

Les dossiers de preuve doivent être archivés par l'expéditeur et/ou le destinataire dans des conditions strictes, régies notamment par la norme AFNOR NF Z42-013, qui a pris effet le 4 mars 2009.

Il est également possible de faire appel aux services d'un tiers archiveur.

#### 1.2.5 SIGNATURE CERTIFIEE

La directive européenne n°1999/93/CE du 13 décembre 1999, la loi n°2000-230 du 13 mars 2000 et son décret d'application n°2001-272 du 30 mars 2001, définissent notamment quatre notions fondamentales :

1. La qualification des prestataires de certification (PSCE), c'est-à-dire l'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité, détaillées dans l'article 6.II du décret. L'arrêté du 26 juillet 2004 décrit le schéma national de qualification des PSCE.
2. Le certificat électronique qualifié, certificat électronique qui doit répondre à des exigences de sécurité et de fiabilité, exposées dans l'article 6.I du décret.
3. Le dispositif de signature sécurisée, qui doit répondre aux exigences du I de l'article 3 du décret. Les dispositifs de signature sécurisée peuvent être certifiés dans les conditions prévues au décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. La délivrance du certificat de conformité est rendue publique.
4. La signature présumée fiable, lorsqu'elle est établie par un dispositif de signature certifié, à l'aide d'un certificat qualifié.

La présomption de fiabilité d'une signature certifiée suppose que la charge de la preuve incombe à l'organisme qui conteste la signature. Dans le cas contraire, la charge de la preuve de la fiabilité du procédé revient au signataire.

L'article 9.III de l'ordonnance du 8 décembre 2005 étend le principe de qualification introduit ci-avant : *« Les produits de sécurité et les prestataires de services de confiance peuvent obtenir une qualification qui atteste de leur conformité à un niveau de sécurité du référentiel général de sécurité. Un décret précise les conditions de délivrance de cette qualification. Cette délivrance peut, s'agissant des prestataires de services de confiance, être confiée à un organisme privé habilité à cet effet ».*

La qualification comporte trois niveaux :

- Élémentaire : ce niveau est noté « une étoile » (\*)
- Standard : noté « deux étoiles » (\*\*)
- Elevé : noté « trois étoiles » (\*\*\*)

Plus le niveau est élevé, plus les exigences de sécurité et de robustesse sont grandes, et plus la garantie apportée par la qualification est significative.

Par ailleurs, chaque niveau de sécurité constituant un sur-ensemble du niveau inférieur, un dispositif de niveau trois étoiles (\*\*\*) peut être utilisé pour toute transaction requérant un niveau une étoile (\*) ou deux étoiles (\*\*).

Les exigences techniques des certificats qualifiés permettant de générer des signatures présumées fiables au sens du décret n° 2001-272 et définies dans l'arrêté du 26 juillet 2004 sont un sous-ensemble des exigences techniques et des règles de sécurité devant être respectées pour être conforme au niveau trois étoiles (\*\*\*) de qualification, au termes de l'article 9.III de l'ordonnance du 8 décembre 2005.

*De ce fait, une signature électronique générée avec un système informatique de signature certifié, et avec des certificats électroniques conformes au niveau trois étoiles (\*\*\*) du référentiel général de sécurité, est conforme au décret n°2001-272, ainsi qu'à la directive européenne 1999/93 CE.*

## 1.3 PRECONISATIONS

### 1.3.1 NORMES ET STANDARDS UTILISES DANS LES PRODUITS DE SECURITE

GU 1. Les produits de sécurité présents dans le système d'information du guichet unique, des prestataires d'aide et ceux utilisés par les prestataires de services de confiance intervenant pour leurs comptes, s'appuient si possible sur des normes et des standards recommandés par le RGS.

### 1.3.2 DOCUMENTS ET INFORMATIONS DELIVRES PAR LE GUICHET UNIQUE EN REPONSE A UNE DEMANDE DE RENSEIGNEMENT

GU 2. Tous les documents et/ou informations délivrés aux déclarants par le guichet unique, ou par un prestataire d'aide en réponse à une demande d'information, sont cachetés (signés) et horodatés, en vue d'un archivage à valeur probante.

GU 3. Les serveurs du guichet unique et ceux des prestataires d'aide utilisent, pour le cachet serveur, des certificats qualifiés de niveau RGS une étoile (\*) selon les conditions du RGS / PRIS V2.2.

GU 4. Les personnels (personnes physiques) du guichet unique et des prestataires d'aide utilisent, pour les opérations d'authentification et de signature électronique, des certificats PRIS ou RGS de niveau deux étoiles (\*\*).

GU 5. En cas de recours à des services de confiance externalisés (par exemple, horodatage ou archivage), le guichet unique et les prestataires d'aide font appel, à chaque fois que c'est possible, à des prestataires qualifiés, au sens de l'arrêté du 26 juillet 2004, et selon les préconisations du RGS / PRIS V2.2.

GU 6. Chaque transaction aboutissant à la délivrance de documents ou d'informations adressées aux déclarants est identifiée de manière unique. L'entité responsable de la transaction (guichet unique ou prestataire d'aide) en garantit la persistance, la consistance, et l'unicité sur une durée d'au moins 5 années.

GU 7. Le numéro d'identification unique est composé de 14 caractères dont les 8 premiers mentionnent l'année, le mois et le jour de sa transmission, les 5 suivants correspondent à un numéro de chrono et le dernier caractère est une lettre permettant d'identifier l'émetteur (guichet unique, prestataires d'aide, mairie). La lettre sera attribuée par le Guichet unique.

GU 8. Un dossier de preuve électronique est constitué pour chaque transaction. Ce dossier est archivé dans des conditions conformes aux recommandations de la norme AFNOR NF Z42-013.

GU 9. Le recours à des tiers de confiance qualifiés est possible, conseillé, mais non obligatoire.

### **1.3.3 CAS DES DECLARANTS**

GU 10. L'authentification des déclarants se fait par simple saisie d'un identifiant et d'un mot de passe « statique ».

GU 11. Le déclarant dispose de la capacité de créer son « compte utilisateur » directement en ligne, sur le site internet du guichet unique ou le cas échéant sur le site du prestataire d'aide.

GU 12. Des fonctions de type « Captcha<sup>5</sup> » ou envoi d'une demande de confirmation par email, sont mises en œuvre, et permettent d'éviter des enregistrements intempestifs par les robots ou autres automates qui circulent sur le Net.

### **1.3.4 CAS DES PRESTATAIRES D'AIDE**

Les prestataires d'aide ayant passé contrat avec le guichet unique sont autorisés à effectuer, pour le compte de leur client, les demandes de renseignements auprès du guichet unique.

Ils disposent pour cela d'un accès complet aux services de bases données exploitants, (discrimination communale et infra communale si cette dernière est disponible) soit par requête directe, soit par la mise à disposition de répliques partiels ou totaux.

Afin de remplir leurs obligations prévues dans l'article 8 de l'arrêté du 23 décembre 2010, les prestataires d'aide peuvent s'ils le souhaitent inclure un lien explicite vers l'adresse « [reseaux-et-canalizations.gouv.fr](http://reseaux-et-canalizations.gouv.fr) ».

L'utilisation d'une balise de type <frame> n'est pas conseillée pour des raisons de conformité au RGAA

GU 13. Cas d'une requête directe (par web service) aux services de bases de données du guichet unique :

- a. Le prestataire exécute, le cas échéant, et sous sa responsabilité, le géocodage. Cette opération est faite en respectant des procédures qualité approuvées par le guichet unique, et à l'aide de référentiels approuvés par le guichet unique.
- b. Le prestataire adresse la requête au guichet unique, via une liaison informatique sécurisée (cf. paragraphe 3.2.2).
- c. Le guichet unique *reçoit la requête*, en *accuse réception*, via une liaison informatique sécurisée, puis procède aux calculs permettant d'identifier les exploitants concernés par le chantier.

---

<sup>5</sup> Un captcha est une forme simple de test de Turing permettant de différencier de manière automatisée un utilisateur humain d'un programme d'ordinateur. La vérification utilise les capacités d'analyse d'image de l'être humain, qui doit taper des lettres et des chiffres visibles sur une image distordue à l'écran.

- d. Le guichet unique prépare la réponse signée et horodatée, et la renvoie au prestataire d'aide, via une liaison informatique sécurisée.
- e. Le guichet unique attribue le numéro unique à la transaction et gère la création, puis l'archivage, du dossier de preuve électronique. En cela, *il endosse la responsabilité de la transaction.*
- f. Il appartient au prestataire de faire parvenir à son client, et sous sa responsabilité, les informations adressées par le guichet unique, par les moyens qu'il estime les plus appropriés.

GU 14. Cas de l'usage d'un réplica des bases de données du guichet unique :

- a. Le prestataire effectue l'intégralité des traitements informatiques permettant d'identifier les exploitants concernés par le chantier, y compris, le géocodage. Ces opérations sont réalisées en respectant des procédures qualité approuvées par le guichet unique, et à l'aide des référentiels approuvés par le guichet unique.
- b. Il signe et horodate lui-même les documents et les informations destinés au client. Il utilise pour cela des moyens de signature certifiée, réputé fiable au sens du décret n° 2001-272, tel qu'indiqué au GU 3.
- c. Il attribue *un numéro unique* (tel que décrit dans le GU 7) à la transaction, dont il gère la persistance, la consistance, et l'unicité sur une durée d'au moins 5 années, en respectant les procédures qualité approuvées par le guichet unique, et à l'aide des référentiels approuvés par le guichet unique.
- d. Il est en charge de la création et de l'archivage du dossier de preuve électronique. Cette opération est faite en respectant les procédures qualité imposées par le guichet unique, et à l'aide des référentiels désignés par le guichet unique. *Le recours à un tiers archiveur est autorisé.*
- e. *De fait, il endosse la totalité de la responsabilité de la transaction.*
- f. Le transfert des dumps des données des exploitants s'effectue au travers d'une liaison informatique sécurisée.

GU 15. L'authentification des personnes physiques, agissant pour le compte des prestataires d'aide, en vue d'établir une session de travail sécurisée avec les systèmes du guichet unique, requiert l'usage d'un certificat de niveau deux étoiles (\*\*) ou supérieur

Cette authentification est nécessaire pour les activités de consultation, de supervision, et de paramétrage de systèmes de connexion et de synchronisation établis avec le guichet unique.

### **1.3.5 CAS DES EXPLOITANTS ET PROPRIETAIRES D'OUVRAGES**

GU 16. L'authentification des personnes physiques, agissant pour le compte des exploitants et propriétaires d'ouvrage, en vue d'établir une session de travail sécurisée avec les systèmes du guichet unique, requiert l'usage d'un certificat de niveau deux étoiles (\*\*) ou supérieur.

L'authentification est notamment nécessaire pour les actions suivantes :

- La mise à jour, par saisie directe, des données de zonage et/ou des coordonnées des services support des exploitants et/ou propriétaires d'ouvrages.
- Le suivi et le reporting des procédures d'importation et de traitement de ces mêmes données.

GU 17. Les personnels (personnes physiques) agissant pour le compte des exploitants / propriétaires d'ouvrage, utilisent, pour les opérations de signature électronique, des certificats qualifiés de niveau deux étoiles (\*\*) ou supérieur, selon les conditions du RGS / PRIS V2.2.

GU 18. Pour effectuer les opérations de signature électronique venant authentifier et approuver les mises à jour de données (par importation ou mise à jour directe sur les pages internet sécurisées du guichet unique), les personnels (personnes physiques), agissant pour le compte des exploitants / propriétaires d'ouvrage, utilisent les systèmes de signature mis à disposition par le guichet unique sur son extranet sécurisé. L'obtention des certificats est à la charge des exploitants.

## **2. GESTION DES REFERENTIELS**

Le guichet unique devra s'appuyer des bases de données référentielles pour réaliser les opérations nécessaires à son fonctionnement :

GU 19. Les référentiels identifiés et choisis par le guichet unique s'imposent aux exploitants et propriétaires d'ouvrages, et prestataires d'aide ayant passé convention avec le guichet unique. Le guichet unique informera par le biais de son site internet dans les meilleurs délais les exploitants de réseaux de toutes modifications des référentiels.

GU 20. A la date de rédaction du présent document, et nonobstant toute évolution ou mise à jour ultérieure, il est préconisé :

- Pour référentiel des communes, arrondissements, aires-urbaines, cantons, EPCI, départements, et régions : *Code Officiel Géographique*<sup>®</sup> publié par l'INSEE, dans sa version à jour au 1er janvier 2011.
- Pour les bases de données topographiques et foncières : produits de l'Institut Géographique National (IGN), composants du RGE : BD TOPO<sup>®</sup>, BD ADRESSE<sup>®</sup>, BD NYME<sup>®</sup>, BD PARCELLAIRE<sup>®</sup>...
- Le guichet unique informera l'ensemble des exploitants de réseaux par le biais de son site internet de versions de bases de données de l'IGN qu'il utilise et de toutes modifications de ces bases.

### **2.1 GEOCODAGE**

Le géocodage est l'opération consistant à transformer une adresse géographique<sup>6</sup> (ou une plage d'adresses géographiques<sup>7</sup>) en une suite de coordonnées planimétriques ou géographiques, au sein d'un système de référencement déterminé.

---

<sup>6</sup> L'adresse géographique est l'adresse physique de l'entité. C'est la structure d'adresse la plus fréquemment utilisée. Elle s'oppose à l'adresse postale, qui ne contient que des éléments postaux ne permettant pas de localiser géographiquement l'entité (par exemple : Entreprise SA – BP 2 – 01100 Pouilly-les-cactus Cedex).

Le géocodage permet un pré-positionnement géographique de l'emprise du chantier sur le fond de carte approprié.

Lorsque le déclarant utilise les services, et par conséquent, les moyens informatiques d'un prestataire d'aide, c'est le système d'information de ce dernier qui réalise le géocodage.

GU 21. Les systèmes de géocodage utilisés par les prestataires d'aide pour offrir au déclarant un pré-positionnement de la zone des travaux qu'il doit tracer sont approuvés, préalablement à leur emploi, par le guichet unique.

## 2.2 MISE A JOUR DES DONNEES DE ZONAGE DES EXPLOITANTS

L'acquisition des données de zonages des ouvrages, adressées par les exploitants se fera en deux temps :

- *L'acquisition initiale de l'ensemble des données*, à l'occasion de la mise en service de la version correspondante du guichet unique.
- *Les mises à jour*, permettant d'intégrer les ajouts, les démantèlements partiels ou complets, les retraits définitifs, les modifications d'ouvrages, etc.

Il serait souhaitable que les mises à jour soient limitées aux seules données concernées, sans obligation de retransmettre la totalité du réseau de l'opérateur.

Cet objectif implique que les exploitants soient en mesure d'identifier leurs ouvrages de façon univoque dans leur système d'information.

L'identifiant unique pourrait ainsi être transmis en tant que métadonnée associée aux données géographiques délimitant la zone d'implantation d'un ouvrage.

Ainsi, le remplacement des données obsolètes par les nouvelles informations serait grandement facilité.

### En conséquence :

GU 22. Le guichet unique est en capacité d'accepter des identifiants uniques d'ouvrages, si les exploitants sont en mesure de les fournir.

GU 23. Les exploitants garantissent la persistance, la consistance, et l'unicité de leurs identifiants durant une durée minimale de 5 années. En effet, toute anomalie (doublon...) dans l'identification d'un ouvrage se traduira *par un risque majeur pour la qualité des bases de données du guichet unique*.

GU 24. Si un exploitant exploite plus d'un ouvrage la fourniture d'un identifiant unique est obligatoire.

---

<sup>7</sup> La plage d'adresse est pour une même voirie

### **3. FLUX, PROTOCOLES D'ÉCHANGE, FORMATS DE DONNÉES**

#### **3.1 DIAGRAMME DES FLUX**

Le guichet unique se trouve au centre d'un ensemble de flux d'informations échangés entre les différents acteurs, dans l'objectif de réaliser les déclarations réglementaires préalables à tous travaux : déclaration de projet de travaux (DT) et déclaration d'intention de commencer les travaux (DICT).

Les macro-flux sont présentés graphiquement sur le schéma ci-dessous.

**Macro-flux A** : il s'agit des échanges d'informations entre, d'une part, les déclarants et, d'autre part, les sites internet des prestataires d'aide à la réalisation des DT / DICT.

**Macro-flux B** : il s'agit des échanges d'informations entre, d'une part, les serveurs du site Internet du guichet unique, ou les serveurs des prestataires d'aide à la réalisation des DT / DICT, et, d'autre part, les services de bases de données du guichet unique.

**Macro-flux C** : il s'agit des flux d'archivage des dossiers de preuve électronique, établis entre, d'une part, le guichet unique ou les prestataires d'aide à la réalisation des DT / DICT, et, d'autre part, un tiers archiveur qualifié.

**Macro-flux D** : il s'agit des flux d'informations relatifs aux données de zonage et aux coordonnées des services de support, échangés entre, d'une part, les exploitants / propriétaires d'ouvrage, et, d'autre part, le guichet unique.

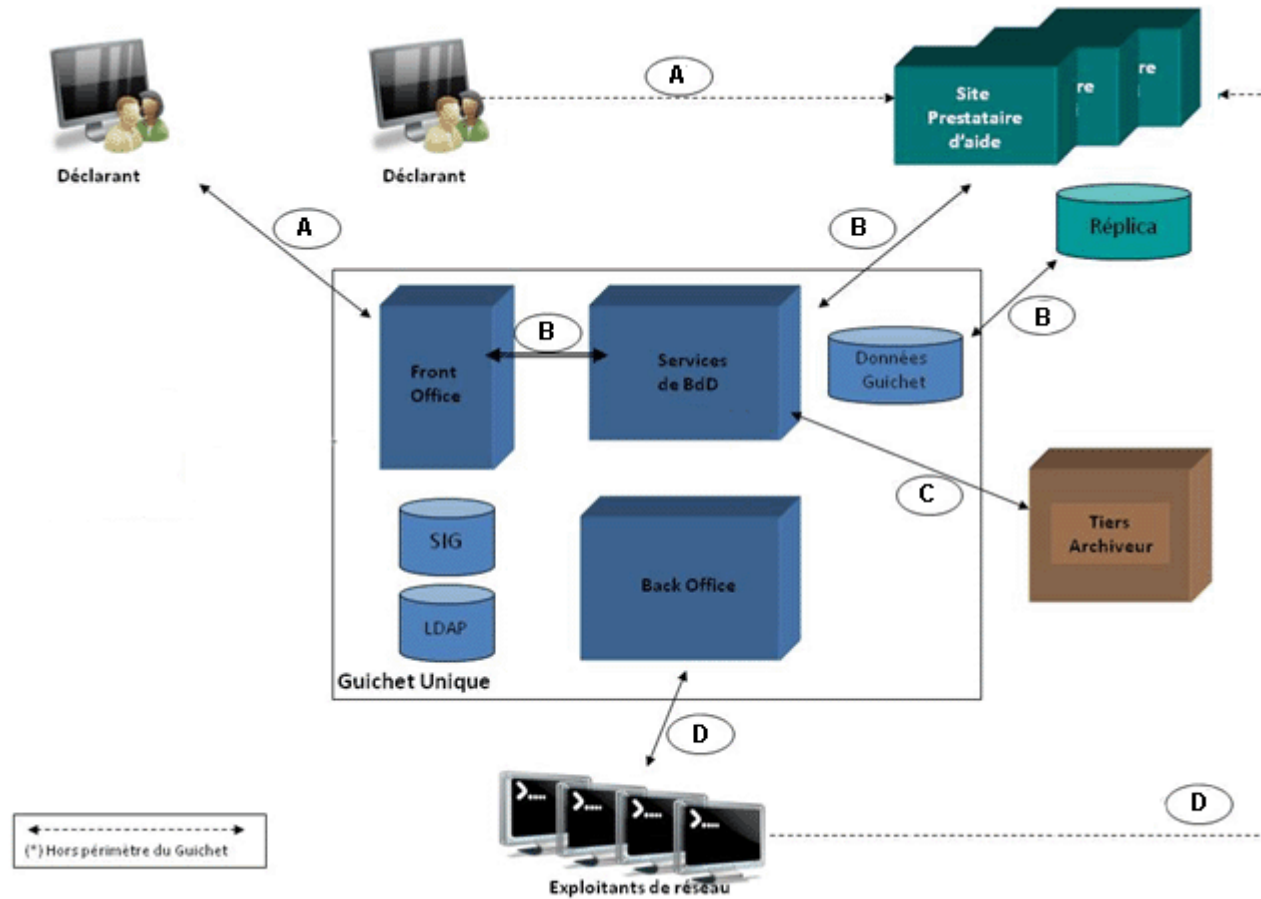


Figure 1 : Présentation des macro-flux d'informations, mis en œuvre dans le processus des échanges de données entre le guichet unique et ses partenaires



### 3.2 FLUX IDENTIFIES POUR LES PRESTATAIRES D'AIDE

#### 3.2.1 MACRO-FLUX A - FLUX ENTRE LE DECLARANT ET LE TELESERVICE

Le macro-flux A se décompose en deux flux élémentaires :

##### 3.2.1.1 FLUX A.1 – REQUETE D'UN DECLARANT

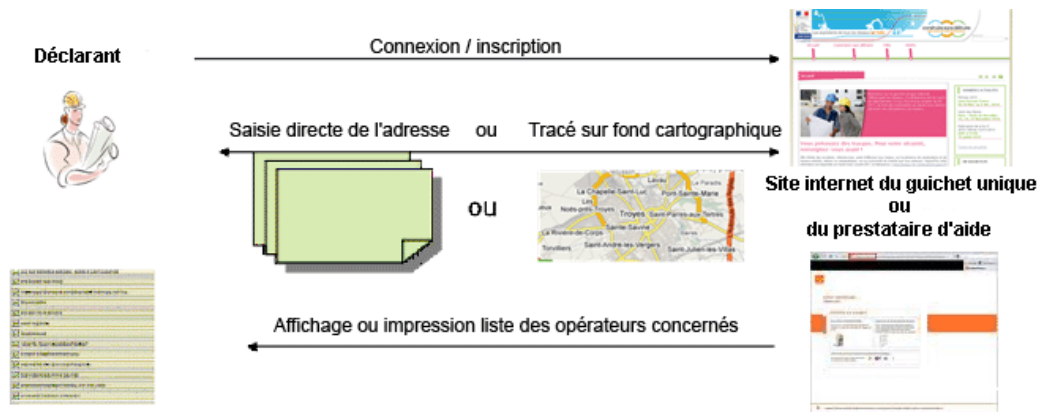


Figure 2 : Présentation du flux A.1

#### Description du flux et protocoles de communication à employer :

- GU 25. Le déclarant établit avec le site Internet du guichet unique ou d'un prestataire d'aide à la réalisation des DT / DICT, un dialogue « requêtes - réponses » WEB HTTP tout à fait classique.
- GU 26. L'utilisation d'un protocole sécurisé HTTPS /TLS est recommandée, mais non obligatoire. Cette option permet un premier niveau de prévention contre le hameçonnage.
- GU 27. La connexion de l'utilisateur, par saisie d'un identifiant et d'un mot de passe est facultative pour la navigation sur le site. Elle est requise lors de l'opération de validation.
- GU 28. Le tracé sur le fond cartographique est affiché via un service de type WMS/WCS publié sur le site du guichet unique ou du prestataire d'aide.
- GU 29. Si le déclarant dispose d'un certificat de signature électronique, acquis pour d'autres téléservices, il pourra à moyen terme, authentifier et signer sa demande.

### 3.2.1.2 FLUX A.2 - TELECHARGEMENT SECURISE DE LA LISTE DES EXPLOITANTS SIGNEE ET HORODATEE

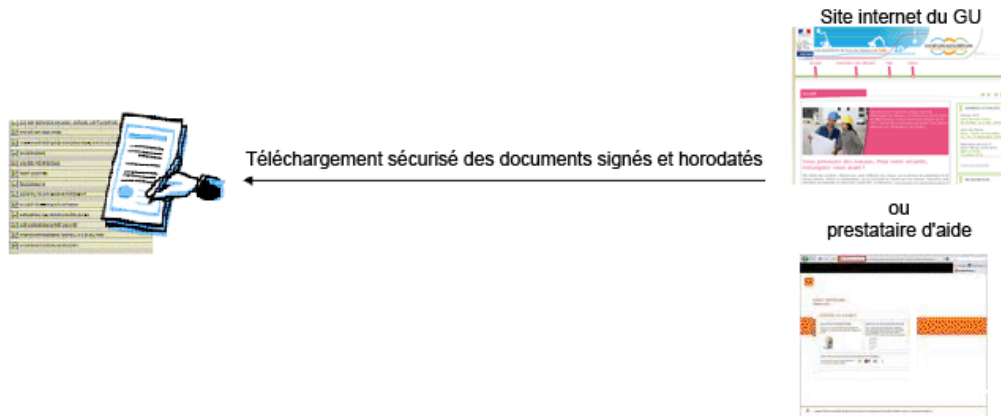


Figure 3 : Présentation du flux A.2

GU 30. Le téléchargement des documents produits par le guichet unique ou le site internet du prestataire d'aide est rendu obligatoire pour le déclarant : les documents signés sont *des originaux numériques* dont l'utilisateur doit impérativement entrer en possession.

GU 31. Le téléchargement est obligatoirement en mode HTTPS / TLS ou SSH, via une solution de téléchargement garantissant la traçabilité.

GU 32. Il est interdit d'envoyer les documents par email, aucune garantie de remise ne pouvant être assurée.

GU 33. Les données adressées au déclarant sont signées et horodatées, lisibles et imprimables par celui-ci, au format PDF *signé*. La signature peut être vérifiée très simplement avec le lecteur ADOBE READER® (version 6 et au-delà).

GU 34. La représentation graphique de l'emprise du chantier n'est pas incluse dans le PDF signé, mais ajoutée comme pièce annexe, pour information. Elle se présente sous la forme d'un fond cartographique à l'échelle 1/5000 (ou moins), bitmap couleur, comportant également les réseaux ferrés et routiers, les ouvrages bâtis, l'hydrographie, les adresses, les toponymes, et la végétation.

### 3.2.2 MACRO-FLUX B - ECHANGE ENTRE LES SERVEURS WEB ET LE SERVICE DE BASE DE DONNEES

Le macro-flux B se décompose en trois flux élémentaires :

- Les « flux B.1 » et « B.2 » sont des échanges « *machine to machine* » entre les serveurs WEB Internet du guichet unique, ou ceux des prestataires d'aide, et les serveurs de bases de données du guichet unique :

- Il est retenu l'hypothèse la plus défavorable pour la description de ces deux flux : les serveurs des différentes parties sont localisés sur des sites distants, sont raccordés à des réseaux distincts, derrière des équipements de sécurité séparés.
- Le « flux B.3 » est un dialogue interactif entre une personne physique agissant pour le compte d'un prestataire d'aide à la réalisation des DT / DICT et le « back office » du guichet unique, c'est-à-dire l'interface Web à partir de laquelle les prestataires et les exploitants peuvent effectuer un certain nombre de tâches techniques.
- Le « flux B.4 » Transfert des dumps entre le guichet unique et les prestataires d'aide.

### 3.2.2.1 FLUX B.1 - CONNEXION AUX SERVICES DE BASES DE DONNEES DU GUICHET UNIQUE

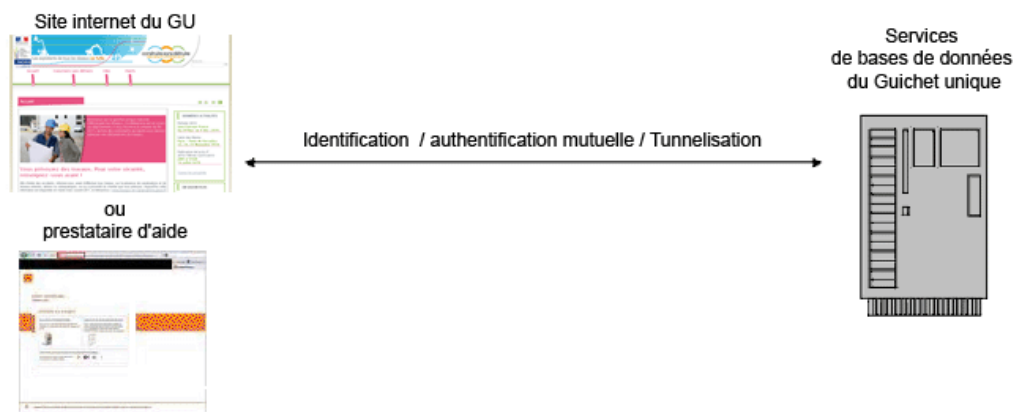


Figure 4 : Présentation du flux B.1

#### Description du flux et protocoles de communication à employer :

GU 35. Il est mis en œuvre, entre, d'une part, les serveurs du prestataire d'aide, et d'autre part, les serveurs des services de bases de données du guichet unique, un tunnel sécurisé :

1. Le tunnel sera un VPN IPSEC, ou, à défaut, un tunnel SSL. Toutefois, ce dernier ne permet pas de faire transiter tous les types de flux réseaux, et peut imposer des contraintes ou des paramétrages spécifiques sur les protocoles mis en œuvre pour échanger les données (notamment SOAP).
2. Ce tunnel IPSEC ou SSL est établi sur une *infrastructure privée d'opérateur*. Cette solution a pour avantage, outre une meilleure sécurité, la maîtrise de la *qualité de service* : garantie de la disponibilité, du débit, du temps de transit, etc.
3. Des équipements de sécurité (IPS, IDS, pare-feu XML...) sont installés à chaque extrémité de réseau. Ces équipements peuvent être mis en œuvre et opérés par l'opérateur de l'infrastructure réseau.

GU 36. La sécurisation du tunnel fait appel à l'échange de clés asymétriques IPSEC / IKE ou SSL, de type RSA 2048 bits. On évitera, *si possible*, les protocoles à secret partagé de type « Diffie-Hellman ».

### 3.2.2.2 FLUX B.2 - ECHANGE D'INFORMATION AVEC LES SERVICES DE BASES DE DONNEES

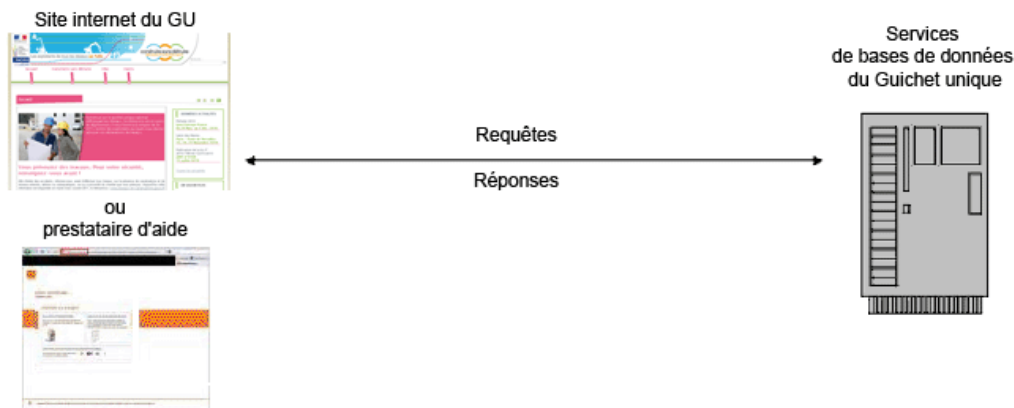


Figure 5 : Présentation du flux B.2

#### Description du flux et protocoles de communication à employer :

GU 37. Les échanges d'informations entre les deux partenaires de la communication ont les caractéristiques suivantes :

- Les requêtes et les réponses sont *d'un haut niveau d'abstraction* : elles ne sont pas liées à un matériel, un logiciel, ou un protocole réseau particulier.
  - Les requêtes contiennent les données relatives aux travaux envisagés par l'utilisateur :
    - Le cas échéant, dans le cas d'une demande d'information sur une DT déjà réalisée, le numéro de consultation unique de la DT et la clé secrète sur 4 chiffres
    - Les coordonnées de l'emprise du chantier, sous forme d'une suite d'objets surfaciques, décrits par leurs coordonnées géographiques, dans un référentiel adapté à la région du chantier.
    - Le géocodage est toujours réalisé par le requérant. Les coordonnées de l'emprise du chantier sont toujours présentes dans la requête.
  - Lorsque l'utilisateur a validé sa requête, les réponses contiennent les documents signés et horodatés, décrits dans le *Flux A.2*
- Pour cette raison, ce flux se trouve « à mi-chemin » entre un échange de documents / messages et un appel à une procédure distante (RPC).
- Les données sont « encapsulées » dans des enveloppes électroniques structurées, de préférence en XML.
- Les échanges sont synchrones ou asynchrones.
- Il doit exister une garantie de remise des informations (requêtes ou réponses) à leur destinataire.
- Les erreurs de transmission sont gérées :

- Un code unique identifie l'erreur.
  - Un libellé donne un message explicatif compréhensible et utile.
  - Un attribut donne une information de sévérité.
- Les services web fournis par les prestataires d'aide au guichet ou aux autres prestataires d'aide, (pour consulter les informations d'une DT déjà réalisée) devront être identiques à ceux du guichet unique de telle manière que les interrogations soient interopérables.

GU 38. Le protocole SOAP (actuellement dans sa version 1.2) est le format nominal retenu pour les échanges décrits précédemment.

GU 39. Le recours à une architecture REST est également autorisé, comme format de repli. Il fait l'objet d'un accord conjoint entre les deux partenaires de la communication.

GU 40. L'implantation du protocole SOAP doit être conforme à la dernière version approuvée du « Basic-profile » (actuellement en version 1.2) par le consortium WS-I.

GU 41. En cas d'utilisation du protocole SOAP, les fonctions exposées par les services de bases de données du guichet unique sont décrites en WSDL v2.0.

GU 42. En cas d'utilisation de REST, il est recommandé, mais non obligatoire, de retenir ATOM comme protocole/format complémentaire.

GU 43. La mise en œuvre d'autres spécifications de Services Web (« WS-\* ») est possible mais non obligatoire. Elle fait l'objet d'un accord conjoint entre les deux partenaires de la communication.

GU 44. Les requêtes destination des services de bases de données du guichet unique, sont encodées comme suit :

- L'emprise du chantier est transmise sous forme d'un ou plusieurs objets surfaciques (polygones) caractérisés par les coordonnées de leurs sommets dans le système de référence géodésique RGF 93.
- Sont acceptées :
  - France métropolitaine et Corse : RGF93
  - Martinique / Guadeloupe : WGS84
  - Réunion : RGR92
  - Guyane : RGFG95
  - Mayotte : RGM04
- Les coordonnées sont géographiques (longitude - latitude) en degrés décimaux.
- Les coordonnées de l'emprise du chantier sont exprimées en XML, conforme aux schémas OGC GML INSPIRE.

- A défaut de GML, il est accepté comme format de repli, lorsque le système de référencement le permet, des données XML conformes au schéma OGC KML 2.2.
- En cas de recours à SOAP, les données binaires sont encapsulées en MTOM/XOP.
- Le codage des caractères est UTF-8.
- Les informations sont exprimées uniquement en Français.
- Les dates prennent la forme AAAA-MM-JJ (AAAA = année sur 4 chiffres, obligatoire ; MM = mois sur 2 chiffres, facultatif ; JJ = jour sur 2 chiffres, facultatif), selon le standard W3CDTF (<http://www.w3.org/TR/NOTE-datetime>) et la norme ISO 8601 (2004).

### 3.2.2.3 FLUX B.3 - INTERVENTION DES PRESTATAIRES D'AIDE SUR LE GUICHET UNIQUE

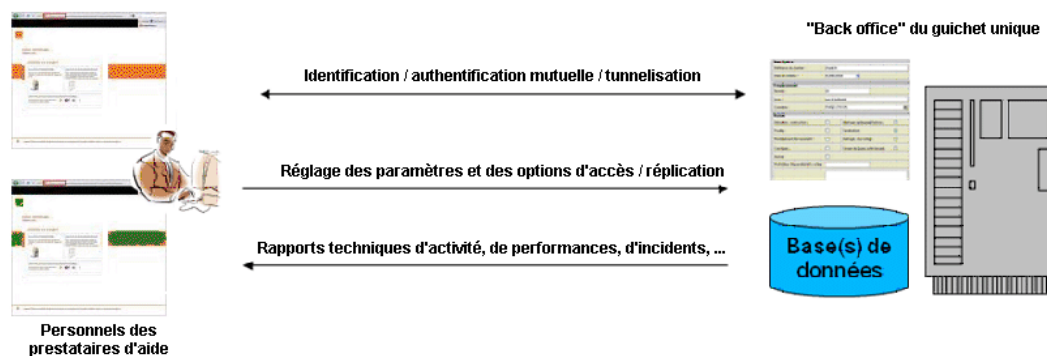


Figure 6 : Présentation du flux B.3

#### Description du flux et protocoles de communication à employer :

Ce flux permet aux personnels techniques des prestataires d'aides de *superviser* (*paramétrage de la connexion, visualiser la disponibilité, les temps de réponse, ...*), et le cas échéant, *d'intervenir* sur le fonctionnement des interfaces informatiques entre leurs propres serveurs et les services de bases de données du guichet unique. Ces réglages techniques peuvent avoir un impact très important sur la fiabilité, la sécurité, et la cohérence des échanges d'informations.

GU 45. Les personnels habilités à réaliser ces interventions sont :

- Identifiés, dans les bases de données du guichet unique.
- Authentifiés, lorsqu'ils se connectent au guichet unique : certificat électronique qualifié de niveau deux étoiles (\*\*) ou supérieur.

GU 46. Le flux est initié par une procédure de connexion avec authentification des deux parties, puis il y a mise en œuvre d'un tunnel HTTPS / TLS.

GU 47. Les données devant être échangées n'étant pas confidentielles, il n'est pas nécessaire de mettre en œuvre un processus de chiffrement. Toutefois, cette option n'est pas interdite ; le protocole à employer est alors AES (128, 192 ou 256 bits).

GU 48. Il n'est pas nécessaire que les informations de supervision envoyées par le guichet unique soient signées électroniquement.

GU 49. Toutes les modifications effectuées sont tracées dans des fichiers journaux, et conservés pendant une durée minimale d'un an au sein du guichet unique, ou auprès d'un tiers qualifié.

### 3.2.2.4 FLUX B.4 – TUNNELISATION ENTRE LE GUICHET UNIQUE ET LES PRESTATAIRES D'AIDE

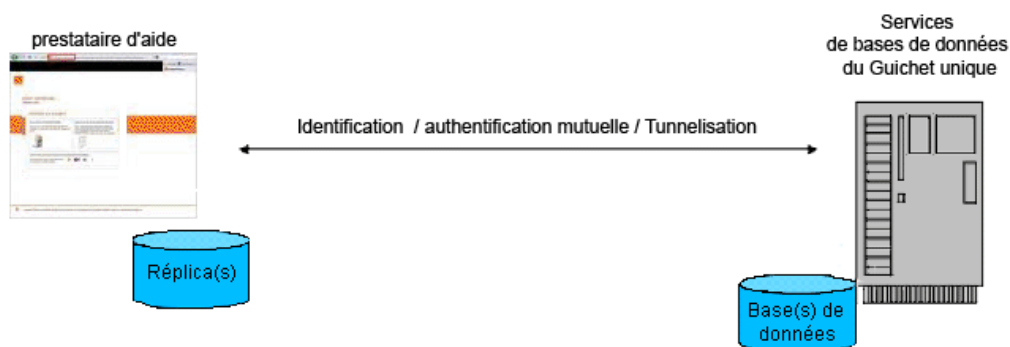


Figure 7: Présentation du flux B.4

#### Description du flux et protocoles de communication à employer :

Ce flux permet de décrire le transfert des dumps entre le guichet unique et les prestataires d'aide.

- Les dumps sont signés par certificat serveur du GU.
- Les dumps sont transférés de façon sécurisé et déposés chaque semaine par le GU chez les prestataires d'aide.
- Le prestataire d'aide accuse réception des dumps.
- Archivage de la preuve du bon téléchargement (ou de la bonne réception) des dumps.
- Les dumps constituent le réplica partiel de la base de données contact/commune/polygone, en fonction du territoire (région) du prestataire.

### 3.2.3 MACRO-FLUX C - INFORMATIONS ECHANGEES AVEC UN ORGANISME TIERS ARCHIVEUR

Le macro-flux C correspond aux informations échangées avec un organisme tiers archiveur.

Le macro-flux se décompose en deux flux élémentaires :

### 3.2.3.1 FLUX C.1 - TUNNELISATION AVEC LE TIERS ARCHIVEUR



Figure 8: Présentation du flux C.1

GU 50. S'agissant d'un contrat avec un partenaire externe, les modalités techniques précises de la communication devront être établies conjointement avec le tiers archiveur.



### 3.2.3.2 FLUX C.2 - ARCHIVAGE DES DOSSIERS DE PREUVE ELECTRONIQUE

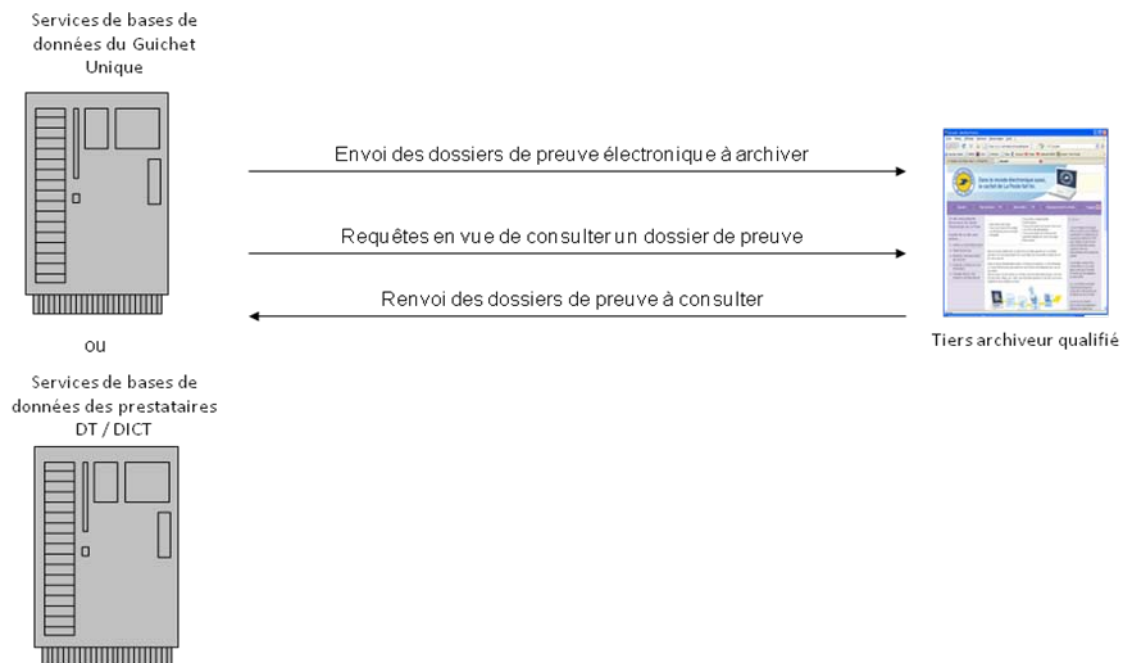


Figure 9 : Présentation du flux C.2

Ce flux comprend les opérations suivantes :

- Création d'un dossier de preuve.
- Ajout de documents dans un dossier de preuve existant.
- Ajout de signatures.
- Fermeture d'un dossier de preuve.
- Demande d'un dossier de preuve, et/ou opérations associées.
- Demande d'un document extrait d'un dossier de preuves.
- Etc.

GU 51. Le protocole de communication, ainsi que les formats de données, seront décidés conjointement avec le tiers archiveur sélectionné.

## 3.3 FLUX IDENTIFIES POUR L'EXPLOITANT DE RESEAUX

### 3.3.1 MACRO-FLUX N° D - MISE A JOUR DES DONNEES DES EXPLOITANTS

La mise à jour des données de zonage des ouvrages et des coordonnées de services support peut se faire de trois façons :

1. Mise à jour directe par un opérateur humain *via* l'interface Web du « Back-Office » du guichet unique (flux D.1).
2. « Upload », c'est-à-dire le *téléchargement ascendant* de fichiers sur le sas d'acquisition du « Back-Office » (flux D.2).
3. Autre cas : Impossibilité de mise à jour directe ou d'utiliser le mode lot (flux D.3)

### 3.3.1.1 FLUX D.1 – MISE A JOUR MANUELLE DES DONNEES PAR L'EXPLOITANT

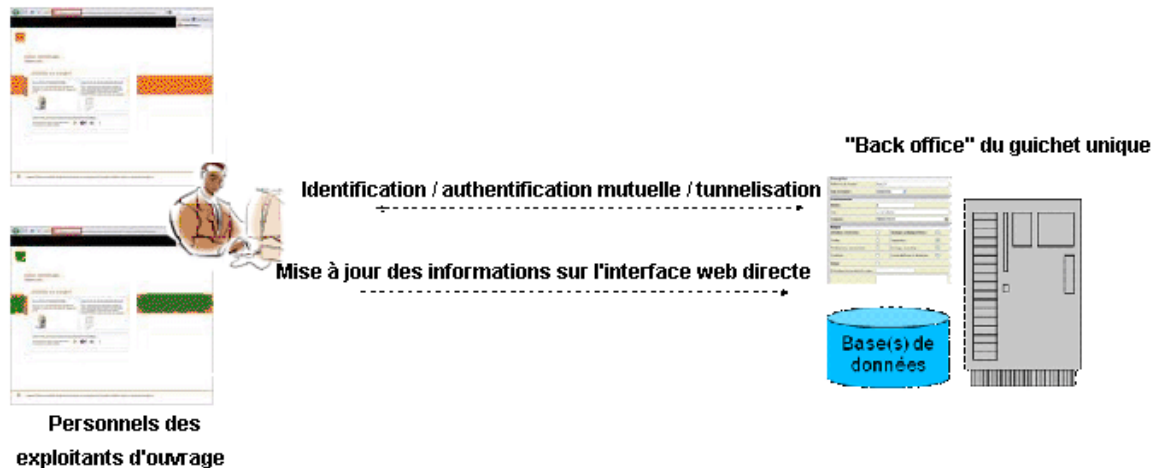


Figure 10 : Présentation du flux D.1

GU 52. Les personnels des exploitants se connectant au « back-office » du guichet unique :

1. Sont identifiés dans une base de données mis en œuvre par le guichet unique.
2. Utilisent des certificats d'authentification de niveau deux étoiles (\*\*) ou supérieur,

GU 53. Le flux est initié par une procédure de connexion avec authentification forte des deux parties, puis mise en œuvre d'un tunnel HTTPS / TLS.

GU 54. Les données devant être échangées n'étant pas confidentielles, il n'est pas nécessaire de mettre en œuvre un processus de chiffrement. Si, toutefois, ce choix était finalement retenu, le protocole à employer est AES (128, 192 ou 256 bits).

GU 55. Toutes les modifications effectuées sont tracées dans des fichiers journaux, et conservés pendant une durée minimale d'un an au sein du guichet unique, ou auprès d'un tiers qualifié. Les exploitants peuvent accéder à l'historique de leurs modifications sur simple demande.

GU 56. Les données saisies directement font l'objet d'un traitement, exécuté par le guichet unique, visant à vérifier la consistance et le formalisme des données. Ce traitement est effectué, si possible, en temps réel. S'il est exécuté en temps différé, des dispositions sont prises pour notifier la fin de ce traitement aux différentes parties. Un dossier de preuves est établi et archivé par le guichet unique.

GU 57. Le détail du processus de traitement des données, aboutissant à leur validation, est défini dans le cadre de la procédure d'assurance-qualité établie par le guichet unique, attachée aux informations fournies par les exploitants et propriétaires d'ouvrages.

GU 58. Le processus de traitement des données s'achève par une phase de validation. L'exploitant vérifie l'intégration correcte des données transmises. Cette phase est matérialisée par un procès-verbal électronique, signé électroniquement par les deux parties.

GU 59. La signature électronique est réalisée à l'aide de certificat de signature de niveau deux étoiles (\*\*) ou supérieur. Pour le guichet unique recours à un cachet serveur.

### 3.3.1.2 FLUX D.2 – MISE A JOUR DES DONNEES DE L'EXPLOITANT PAR UPLOAD DE FICHIER

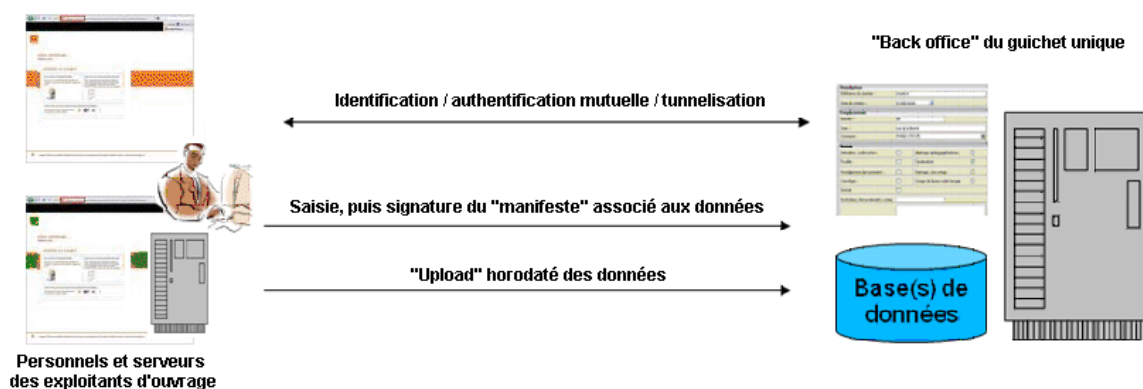


Figure 11 : Présentation du flux D.2

GU 60. Le téléchargement ascendant (« upload ») d'un fichier de données est initié par une personne physique agissant pour le compte de l'exploitant. L'initiation de cet upload par des équipements logiciels installés sur des serveurs, dûment identifiés, appartenant à ce dernier peut être réalisé dans le cadre d'une prestation complémentaire passée avec le guichet unique.

GU 61. Dans tous les cas, une authentification forte est nécessaire pour sécuriser la transaction. Les personnes physiques sont authentifiées par des certificats de niveau deux étoiles (\*\*) ou supérieur.

GU 62. Une fois la connexion établie, l'agent (personne physique ou logiciel) qui s'apprête à « uploader » le fichier de données, remplit le manifeste électronique. Le manifeste est un formulaire électronique qui indique :

- La taille et le format du fichier à télécharger.
- Un identifiant unique pour ce lot de données.
- Le cas échéant, le type d'opération attendu : mise à jour, changement de statut d'un ouvrage, etc.

- Le cas échéant, les formats, schémas, ou référentiels (établis par le guichet unique) auxquels il convient de se référer pour le contrôle qualité des données.
- Et d'une façon plus générale, toutes les informations nécessaires à la bonne acquisition et au bon traitement des données téléchargées.

GU 63. Le manifeste est signé électroniquement par l'agent (personne physique ou logiciel) qui l'a établi.

GU 64. Une fois le téléchargement terminé, le guichet unique adresse une preuve de dépôt électronique signée et horodatée, indiquant que le téléchargement s'est bien passé, et que les données sont bien acquises. Cette preuve de dépôt ne signifie pas que les données sont conformes et consistantes.

GU 65. Les données importées font l'objet d'un traitement, exécuté par le guichet unique, visant à vérifier la consistance et le formalisme des données. Ce traitement est effectué, si possible, en temps réel. S'il est exécuté en temps différé, des dispositions sont prises pour notifier la fin de ce traitement aux différentes parties.

GU 66. Le suivi du processus de traitement des données, aboutissant à leur validation, entre dans le cadre de la procédure d'assurance-qualité établie par guichet unique, attachée aux informations fournies par les exploitants et propriétaires d'ouvrages.

GU 67. Le processus de traitement des données s'achève par une phase de validation. L'exploitant vérifie l'intégration correcte des données transmises. Cette phase est matérialisée par un procès-verbal électronique, signé par les deux parties. L'exploitant doit valider un échantillon de ses données. A cet effet, il pourra, s'il les a communiquées, visualiser ses zones d'implantation sur un fond de plan. La signature du procès verbal par les 2 parties conduit à l'intégration des données. Celles-ci seront accessibles à la consultation lors de la mise à jour suivante. Dans le cas contraire les données ne seront pas mises en ligne.

GU 68. La signature du procès verbal par l'exploitant ne peut être effectuée par un agent logiciel : une personne physique habilitée est obligatoire.

GU 69. La signature du procès verbal est réalisée à l'aide de certificats de signature de niveau deux étoiles (\*\*), ou supérieur (cachet serveur pour le guichet unique).

GU 70. Un dossier de preuves est établi et archivé par le guichet unique.

#### **Format des données fournies par les exploitants et propriétaires d'ouvrages :**

GU 71. Le guichet unique établit, maintient, fait connaître et appliquer, un schéma XML qui lui est propre, pour les données ne disposant pas de schémas standards de référence. Ce schéma est matérialisé par un espace de nommage (Namespace) XML spécifique : « `xsi:type="guichetunique:nom` »

GU 72. Les coordonnées des services support respectent le format suivant :

1. Il est créé, maintenu, et diffusé par le guichet unique un Modèle de fichier CSV dans laquelle les exploitants et/ou les propriétaires pourront enregistrer les informations prévues.
2. Le codage des caractères est *UTF-8*.
3. Les informations seront exprimées uniquement en Français.

GU 73. Les données de zonage respectent le format suivant :

1. Format nominal : fichiers XML conforme aux schémas OGC GML INSPIRE., décrivant des objets surfaciques (polygones) caractérisés par les coordonnées de leurs sommets, et comprenant la mention :
  - De *l'ellipsoïde de référence*, par exemple « *IAG GRS 1980<sup>8</sup>* »
  - Le *système géodésique utilisé est le RGF93*.
  - Sont acceptées :
    - France métropolitaine et Corse : RGF93
    - Martinique / Guadeloupe : WGS84
    - Réunion : RGR92
    - Guyane : RGFG95
    - Mayotte : RGM04
  - Les coordonnées seront géographiques (longitude - latitude) en degrés décimaux.
2. Format de repli : fichiers XML conformes au schéma OGC KML 2.2, décrivant des polygones caractérisés par les coordonnées géographiques de leurs sommets, exprimées en WGS84 - degrés décimaux.
3. Format de repli : fichiers *ShapeFile* ou *MIF/MID* ou, en dernier recours, textuels (DXF), présentant les mêmes caractéristiques qu'en 1.
4. Métadonnées comprises dans les formats décrits, ou sous forme de fichier détaché XML au format ISO 19115 / ISO 19139.

### 3.3.1.3 *FLUX D.3 – AUTRE CAS : IMPOSSIBILITE DE MISE A JOUR DIRECTE OU D'UTILISER LE MODE LOT*

GU 74. Dans le cas où l'exploitant de réseaux ne peut pour un ouvrage donné fournir au téléservice les informations nécessaires par saisie directe par upload ou sous un format numérique défini dans le flux D2, il pourra contre rémunération faire appel aux services du guichet unique ou à ceux d'un prestataire d'aide.

## **4. INDEX DES FIGURES ET DES TABLEAUX**

<i>Figure 1 : Présentation des macro-flux d'informations, mis en œuvre dans le processus des échanges de données entre le guichet unique et ses partenaires.....</i>	<i>16</i>
<i>Figure 2 : Présentation du flux A.1.....</i>	<i>17</i>
<i>Figure 3 : Présentation du flux A.2.....</i>	<i>18</i>
<i>Figure 4 : Présentation du flux B.1.....</i>	<i>19</i>
<i>Figure 5 : Présentation du flux B.2.....</i>	<i>20</i>
<i>Figure 6 : Présentation du flux B.3.....</i>	<i>22</i>
<i>Figure 7 : Présentation du flux B.4.....</i>	<i>23</i>
<i>Figure 8 : Présentation du flux C.1.....</i>	<i>24</i>
<i>Figure 9 : Présentation du flux C.2.....</i>	<i>25</i>
<i>Figure 10 : Présentation du flux D.1.....</i>	<i>26</i>
<i>Figure 11 : Présentation du flux D.2.....</i>	<i>27</i>



*maîtriser le risque |  
pour un développement durable*

**Institut National de l'Environnement Industriel et des Risques**

Parc technologique alata - BP 2 - 60550 Verneuil-en-Halatte

Tél. : +33(0)3 44 55 66 77 - Fax : +33(0)3 44 55 66 99

E-mail : [ineris@ineris.fr](mailto:ineris@ineris.fr) - Internet : [www.ineris.fr](http://www.ineris.fr)